

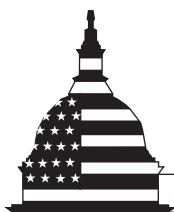
GAO

Report to the Ranking Member,
Subcommittee on Crime, Terrorism,
and Homeland Security, Committee on
the Judiciary, House of Representatives

June 2011

ORGANIZED RETAIL CRIME

Private Sector and Law Enforcement Collaborate to Deter and Investigate Theft



G A O

Accountability * Integrity * Reliability

Highlights of [GAO-11-675](#), a report to the Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

Each year organized groups of professional shoplifters steal or fraudulently obtain billions of dollars in merchandise to resell in an activity known as organized retail crime (ORC). These stolen goods can also be sold on online marketplaces, a practice known as “e-fencing.” GAO was asked to assess ORC and e-fencing. This report addresses: (1) types of efforts that select retailers, state and local law enforcement, and federal agencies are undertaking to combat ORC; (2) the extent to which tools or mechanisms exist to facilitate collaboration and information sharing among these ORC stakeholders; and (3) steps that select online marketplaces have taken to combat ORC and e-fencing, and additional actions, if any, retailers and law enforcement think may enhance these efforts. GAO reviewed retail-industry documentation, such as reports and surveys, and academic studies related to ORC and efforts to combat it. GAO also interviewed representatives from four major retail associations and five individual retailers, selected for their knowledge of and efforts to combat ORC, as well as eight local law enforcement officials involved in the development of ORC information sharing networks, and Federal Bureau of Investigation (FBI) and U.S. Immigration and Customs Enforcement (ICE) officials. The results are not generalizable, but provided insights on activities related to ORC. GAO is not making any recommendations in this report.

View [GAO-11-675](#) or key components.
For more information, contact Eileen Larence
at (202) 512-8777 or larencee@gao.gov.

June 2011

ORGANIZED RETAIL CRIME

Private Sector and Law Enforcement Collaborate to Deter and Investigate Theft

What GAO Found

Retailers collaborate with law enforcement agencies to detect and deter retail theft and investigate potential ORC cases, and federal agencies are taking steps to better track their involvement. Stopping ORC begins with retailers, which have invested in new technologies and personnel to deter and investigate ORC. These investigations are often conducted in concert with local law enforcement, which generally must balance ORC investigative demands with other offenses—including violent crime. Federal agencies, including FBI and ICE, also work major ORC cases in conjunction with retailers and local law enforcement. These agencies do not have dedicated ORC resources, but both have implemented recent efforts to enhance tracking of ORC cases within their case management systems, including developing a program code to better track involvement in ORC cases. Such tracking is intended, in part, to improve data collection and reporting of case information and help inform management resource decisions.

Emerging regional networks are facilitating information sharing among ORC stakeholders including retailers and law enforcement, but limitations were cited with the existing national database. Officials from all eight of the local law enforcement entities GAO interviewed have, with retail partners, established regional networks in recent years to facilitate information sharing among stakeholders and identify linkages between connected retail theft cases. A national database, which was created by the retail community with input provided by the FBI based on a legislative mandate, also exists to share ORC information. However, all five retailers GAO interviewed reported concerns related to the database’s functionality, such as missing analytics to help retailers or law enforcement identify trends. In April 2011, the system was acquired by a company with experience managing large information-sharing databases in several major industries. According to the owner, when the new system becomes operational in the summer of 2011, it will include a series of enhancements intended to address the key concerns identified. It is too soon to tell to what extent retailers will expend resources to utilize an enhanced national ORC database.

Leading online marketplaces have taken steps to combat ORC and e-fencing, but it is unclear if additional federal action would further deter this practice. eBay, the largest online marketplace, has recently taken steps to deter e-fencing, but varying business models and available resources may impact efforts of other online marketplaces. Efforts by eBay are designed to make it more responsive to requests for information from both retailers and law enforcement, both of which usually need seller information to link stolen merchandise to specific people. Retail and law enforcement stakeholders GAO interviewed identified two options—both imposing restrictions on sellers using online marketplaces—they felt could help combat ORC. However, these options would require legislative changes to implement, and it is unknown what deterrent effect the options may have on ORC and e-fencing.

In commenting on a draft copy of this report, DOJ and DHS provided technical clarifications, which GAO incorporated where appropriate.

Contents

Letter		1
	Background	5
	Retailers and Law Enforcement Collaborate to Investigate Potential ORC Cases, and Federal Agencies Are Taking Steps to Better Track ORC	10
	Emerging Regional Networks Are Facilitating Information Sharing among ORC Stakeholders, but Limitations Exist with National ORC Database	24
	Leading Online Marketplaces Have Taken Steps to Combat e-Fencing, but It Is Unclear If Additional Federal Action Is Warranted	30
	Agency Comments and Our Evaluation	40
Appendix I	Comments from the Department of Homeland Security	42
Appendix II	GAO Contact and Staff Acknowledgments	44
Tables		
	Table 1: Summary of Select Efforts Employed by Retailers to Combat Organized Retail Crime	14
	Table 2: Characteristics of Selected Regional Networks Targeting Organized Retail Crime	25
Figures		
	Figure 1: Organized Retail Crime Life Cycle	8
	Figure 2: Select Technologies to Deter Retail Theft	12

Abbreviations

ARAPA	Albuquerque Retail Assets Protection Association
BAORCA	Bay Area Organized Retail Crime Association
CCROC	Cook County Regional Organized Crime Task Force
CPI	Crime Problem Indicator
ECPA	Electronic Communications Privacy Act
EU	European Union
FBI	Federal Bureau of Investigation
FORCE	Florida Organized Retail Crime Enforcement Network
ICE	U.S. Immigration and U.S. Customs Enforcement
LAAORCA	Los Angeles Area Organized Retail Crime Association
LERPnet	Law Enforcement and Retail Partnership network
LPRC	Loss Prevention Research Council
ORC	organized retail crime
OTC	over the counter
SDORCA	San Diego Organized Retail Crime Association
SEARCH	Seizing Earnings and Assets from Retail Heists
USSS	U.S. Secret Service
WSORCA	Washington State Organized Retail Crime Association

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

June 14, 2011

The Honorable Robert C. Scott
Ranking Member
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
House of Representatives

Dear Mr. Scott:

Each year organized groups of professional shoplifters steal or fraudulently obtain billions of dollars in retail merchandise to resell into the marketplace. This activity, known as organized retail crime (ORC), is a growing concern for retailers nationwide and the law enforcement entities responsible for investigating and prosecuting these offenses. In addition to the direct financial losses to retailers and reduced state tax revenues, ORC also presents potential public health and safety concerns. For example, some products commonly stolen for resale include infant formula, over-the-counter medications, and other health and beauty items, which may be potentially expired, repackaged, or improperly stored or handled before reaching the consumer. In addition to traditional resale venues, such as flea markets and pawn shops, ORC groups have increasingly turned to online marketplaces to sell (or “fence”) their stolen goods to a wider audience, a practice known as e-fencing.¹

ORC routinely spans multiple jurisdictions, and combating this activity involves coordination among a variety of different stakeholders including retailers and state, local, and federal law enforcement, as well as operators of online marketplaces such as eBay and Amazon. The Federal Bureau of Investigation (FBI) is the primary federal agency involved in major ORC investigations, but other agencies including US Immigration and Customs Enforcement (ICE) and the US Secret Service (USSS) may also play a role as ORC can have a transnational component or involve money laundering. Given the potential impact of ORC and the unique challenges posed by e-fencing, Members of Congress have also introduced bills in recent years that include provisions intended to help combat these offenses. These proposals have included, for example, revisions to the U.S. Code

¹ A “fence” is an individual or organization that knowingly purchases stolen or illegally obtained goods for the purpose of reintroducing those goods back into commerce.

identifying ORC as a federal crime, additional requirements for operators of online marketplaces to monitor sellers for potential e-fencing, and authorization of federal resources to investigate and prosecute ORC activities. In response to your request, this report addresses the following questions:

- What types of efforts are select retailers, state and local law enforcement agencies, and federal agencies undertaking to combat organized retail crime?
- To what extent do tools or mechanisms exist to facilitate information sharing and collaboration among stakeholders to combat ORC?
- What steps are select online marketplaces taking to combat ORC and e-fencing, and what additional federal actions, if any, do stakeholders think may enhance these efforts?

To identify the types of efforts stakeholders (i.e., select retailers, state and local law enforcement, and federal agencies) are undertaking to combat ORC, we reviewed retail industry reports, surveys, white papers, and past testimony from congressional hearings on ORC, as well as academic studies, related to organized retail crime and retailer efforts to combat ORC. We also interviewed four major retail associations—including the National Retail Federation, Retail Industry Leaders Association, the Food Marketing Institute, and the National Association of Chain Drug Stores—and five individual retailers, including Target Corporation, Home Depot, Best Buy, SuperValu, and Walgreens. We selected these associations and retailers because they represent different major retail-market segments and provide insight into ORC-related concerns and loss prevention efforts across the retail industry. The specific retailers we selected were identified based on recommendations from the retail associations and the retailers' level of activity in combating ORC. Because we used nonprobability sampling to select the associations and retailers, the information obtained from these interviews cannot be generalized to other retailers. However, the information obtained provided valuable perspectives on ORC and specific examples of efforts underway at five large national retailers. While this report identifies the prevalence of common retailer perspectives where appropriate, certain issues or concerns, such as those related to the theft of specific products, may not be universally applicable given the unique industry segments of some individual retailers. We also interviewed academics from the University of Florida and experts in the field of loss prevention. These experts were selected based on our review of background literature related to ORC, as well as referrals from others in the loss prevention field.

To obtain information on efforts law enforcement stakeholders are undertaking, we interviewed representatives from 10 state and local law enforcement agencies in California, Illinois, Florida, Maryland, New Mexico, and Washington to understand how they work with retailers and federal law enforcement during ORC investigations. Specifically, these agencies included eight local law enforcement jurisdictions and two state agencies. These law enforcement agencies were initially identified by retailers and retail associations and were selected based on prior involvement in ORC cases and in organized regional information-sharing networks designed to share details of ORC incidents among neighboring jurisdictions. The information obtained from these interviews cannot be generalized across all local law enforcement agencies in the United States. However, the interviews provided perspectives and examples of how select law enforcement agencies active in ORC investigations conduct their work in conjunction with other stakeholders. Where applicable, we included information in the report regarding the prevalence of specific issues cited by law enforcement officials; however, the roles and experiences varied among these officials and not all were able to comment on each of the issues presented.

To identify the roles of the federal government in combating ORC, we reviewed relevant testimony from the federal agencies in the past four congressional hearings on ORC and interviewed federal law enforcement officials. We interviewed senior program officials in the headquarters offices of FBI, ICE, and USSS involved in overseeing and investigating ORC cases. These federal agencies were selected because they have historically been the law enforcement agencies primarily involved in investigating ORC-related activity. In addition, we interviewed officials in ICE's Los Angeles field office, one of the locations where an ORC pilot program is underway. The Los Angeles pilot was selected because, according to the National Retail Federation, Los Angeles is an area of substantial ORC activity and local law enforcement is active in the issue. In addition, we spoke with the U.S. Attorney's Office for the Northern District of California, San Jose Branch Office about federal efforts to prosecute ORC cases. The office was selected, in part, because stakeholders identified that two ORC cases were actively being prosecuted by that office. Finally, we interviewed a special agent within the U.S. Department of Agriculture who has experience with investigations regarding the sale and distribution of stolen infant formula to obtain views on the scope of these types of activities and identify potential health and safety related impacts.

To determine the extent to which tools or mechanisms exist to facilitate information sharing and collaboration between ORC stakeholders, we used information obtained from interviews with law enforcement and retailers, and reviewed regional information-sharing networks to determine what kind of information was uploaded, how members joined or were selected, and how incident information was distributed to members to aid in investigations. We also reviewed available documentation, such as descriptive summaries and user agreements, related to the national ORC database—the Law Enforcement and Retail Partnership network (LERPnet)—and received a demonstration of the database’s search and reporting capabilities. We also held discussions with the National Retail Federation, retailers, and law enforcement regarding the development and implementation of this system, its current utilization, and any potential improvements that were identified.

To identify the steps that select online marketplaces are taking to combat e-fencing as an outlet for ORC, we interviewed representatives from four online marketplaces—eBay, Amazon.com, Overstock.com and Craigslist. The marketplaces were selected based on our background research and recommendations from law enforcement and retailer stakeholders that identified these companies as the larger marketplaces and potential e-fencing outlets. When available, we reviewed corporate information, sample reports of suspicious listings, and select case examples to determine the scope of the online marketplaces’ efforts to combat fraud on their sites. Because we used nonprobability sampling to select the online marketplaces, the information obtained from these interviews cannot be generalized to other online marketplaces in the United States; however, the information gathered in the interviews enabled us to describe the efforts of major online marketplaces in combating e-fencing.

To identify additional federal actions that stakeholders think could enhance efforts to combat ORC and e-fencing, we conducted interviews with stakeholders to identify common themes and also reviewed selected state laws and proposed federal legislation related to ORC. In addition, we used information from our interview with a U.S. Department of Agriculture agent to identify any federal concerns regarding health and safety related to the reselling or redistribution of infant formula and other health and beauty products. Finally, we reviewed selected laws that govern “high-volume sellers” on online marketplaces in other countries to understand additional requirements that online marketplaces may be subject to overseas to determine the impact of these laws overseas and the applicability of them domestically.

We conducted this performance audit from May 2010 to June 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

ORC Definition: Although the term ORC is commonly used among the retail industry and state and local law enforcement, it remains difficult to clearly define because it can be comprised of several underlying crimes and is subject to different interpretations by retail and law enforcement stakeholders. While there is a federal definition for “organized retail theft,”² we use the term ORC to refer to a broader set of crimes that can affect retail stakeholders, such as fraud associated with gift cards or product returns. Specifically, under federal law, organized retail theft means

- (1) the violation of a state prohibition on retail merchandise theft or shoplifting, if the violation consists of the theft of quantities of items that would not normally be purchased for personal use or consumption and for the purpose of reselling the items or for reentering the items into commerce;
- (2) the receipt, possession, concealment, bartering, sale, transport, or disposal of any property that is known or should be known to have been taken in violation of paragraph (1); or
- (3) the coordination, organization, or recruitment of persons to undertake the conduct described in paragraph (1) or (2).

At the federal level, law enforcement agencies, such as the FBI, prefer to utilize the term organized retail theft to differentiate between in-store theft and cargo theft, or other fraud related activities, which are categorized as

² Pub. L. No. 109-162, § 1105, 119 Stat. 2960, 3093 (2006). The definition is for purposes of establishing a DOJ/FBI task force to combat organized retail theft and the Law Enforcement and Retail Partnership network (LERPnet), a national database, to be housed and maintained in the private sector, to track and identify where organized retail theft type crimes occur.

distinct crimes.³ However, in addition to shoplifting and traditional retail theft crimes, non-federal stakeholders routinely include acquisition of retail merchandise by fraud or other illegal means as a principal component of ORC. Accordingly, we also included these activities within our definition of ORC, in addition to the activities encompassed by the federal definition of organized retail theft. Despite the definitional variations, however, stakeholders are consistent in identifying a clear distinction between ORC incidents and those perpetrated by opportunistic, amateur shoplifters, who tend to steal merchandise for personal consumption.

ORC Operations (“Boosting”): ORC groups employ a range of methods to illegally obtain retail merchandise. Most commonly, professional shoplifters known as “boosters” steal multiple quantities of targeted items that can be readily sold to “fences,” who in turn resell the goods through legal or illegal channels for financial gain. In some cases, fences provide itemized sheets to boosters indicating specific products desired and the amount that will be paid for them. According to retailers, boosters tend to target products that are small, concealable, and of relatively high value. Some frequently stolen products retailers identified include razor blades, diabetic test strips, infant formula, teeth whitening products, cosmetics, and over-the-counter medications, such as Prilosec. One common method employed by boosters is to conceal merchandise in customized bags that have been modified to help circumvent store security systems. Boosters also often work in groups, commonly utilizing lookouts, distraction methods, and, in some cases, sophisticated hand signs to communicate. Other methods boosters employ include practices such as box stuffing, return fraud, and ticket switching.⁴ ORC activity may also include some level of collusion with store employees, who may participate in theft themselves or could assist thieves by such actions as leaving doors

³ For statistical purposes, the FBI defines cargo theft as the criminal taking of any cargo including, but not limited to, goods, chattels, money, or baggage that constitutes, in whole or in part, a commercial shipment of freight moving in commerce, from any pipeline system, railroad car, motortruck, or other vehicle, or from any tank or storage facility, station house, platform, or depot, or from any vessel or wharf, or from any aircraft, air terminal, airport, aircraft terminal or air navigation facility, or from any intermodal container, intermodal chassis, trailer, container freight station, warehouse, freight distribution facility, or freight consolidation facility.

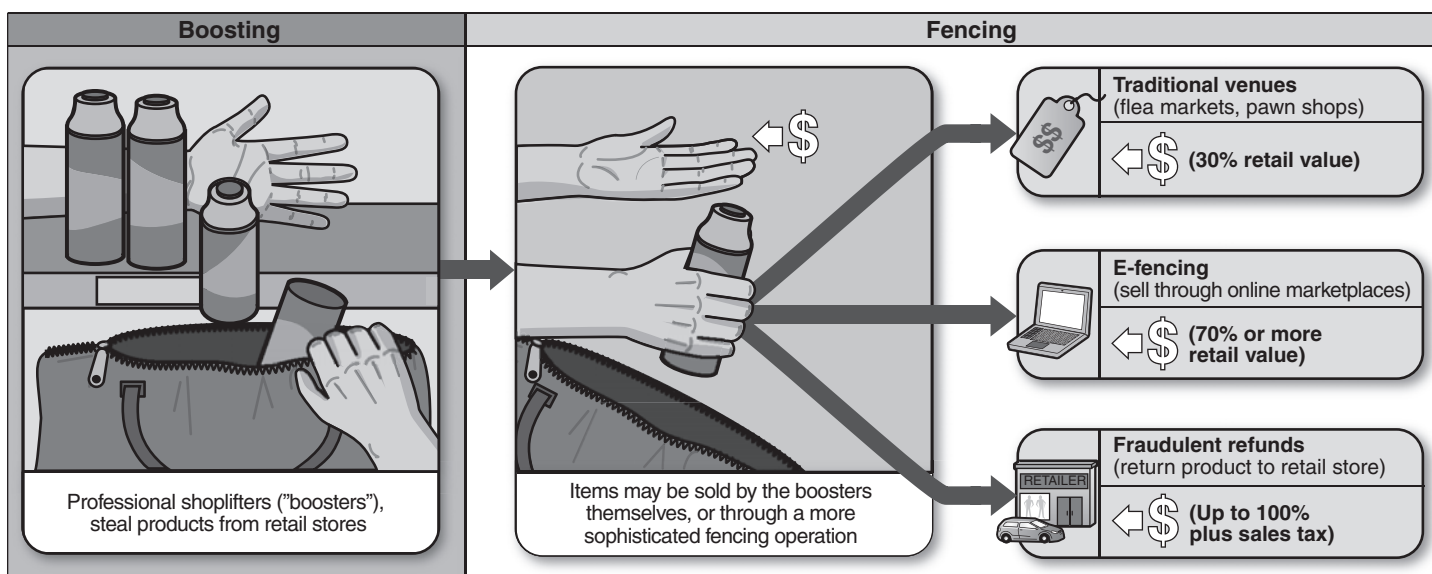
⁴ Box stuffing is the replacing of the contents of one large box with multiple smaller, high-value products. Return fraud occurs when an offender returns an item that was not lawfully acquired to a retail store to obtain cash. Ticket switching occurs when an offender affixes a fraudulent barcode over another so that it rings up at the register at a reduced price.

unlocked or providing alarm codes or other security information. According to retailers, boosters routinely target multiple stores a day, frequently hitting retail stores in shopping malls or near major highways to increase potential targets and allowing a quick escape route.

ORC Operations (“Fencing”): Once retail merchandise is acquired, several different methods are used to fence the products back into the marketplace. Potential outlets for fencing stolen goods include small convenience or second hand stores, flea markets, swap meets, pawn shops, and more recently, online marketplaces. While stolen goods are commonly sold to individual buyers through these venues, in some cases, fencing operations may also employ sophisticated measures to clean and repack products for resale to witting or unwitting wholesale distributors. With the growth of the Internet and online marketplaces, e-fencing in particular has emerged as a major concern for retailers and law enforcement. According to the most recent National Retail Federation survey of retailers, 66 percent of surveyed retailers indicated that they had identified or recovered stolen merchandise and gift cards that were being fenced online.⁵ In contrast to more localized physical fencing operations, e-fencing is generally much more profitable and allows sellers a global reach. For example, retailers indicate that e-fencing can often yield 70 percent or more of the retail value of the product versus approximately 30 percent through traditional fencing venues (see fig. 1). Further, e-fencing eliminates the face-to-face interactions that occur at physical fencing locations, thereby providing sellers with a perceived increase in anonymity.

⁵ National Retail Federation, *Organized Retail Crime Survey* (2010).

Figure 1: Organized Retail Crime Life Cycle



Sources: GAO and NRF.

ORC Impact: Despite widespread recognition that ORC is a significant issue, it remains difficult to precisely estimate the financial impact for many reasons. Numerous press releases and industry reports often cite an estimate of \$15 billion to \$30 billion in annual financial losses attributable to ORC; however, it is unclear how these estimates were developed and neither the FBI nor industry groups were able to identify the sources for these figures.⁶ Even among individual retailers, it remains difficult to estimate the financial impact of ORC in their organizations. For example, retailers can often identify overall inventory losses (shrinkage), but these losses generally come from a number of different sources apart from ORC, including internal employee theft and amateur shoplifting, as well as administrative error or vendor fraud. Since there is rarely a clear audit trail for the cause of shrinkage, retailers typically develop estimates based on professional judgment and the results of prior investigations. Among 100 corporate retail chains that responded to a 2009 retail security survey, an

⁶ Among the potential sources for these estimates are testimonies by senior FBI officials in 2005. The first, delivered in February by FBI Director Robert Mueller, identified annual property losses from cargo, high-tech, and retail theft at an estimated \$30 billion. In March 2005, another senior FBI official cited an estimate of \$15 billion to \$30 billion for organized retail theft losses alone. In 2006, the FBI also estimated financial losses from cargo theft to be \$15 billion to \$30 billion.

average of 11 ORC cases were reported per \$100 million in sales, with an average loss per incident of about \$6,800.⁷ However, given that ORC affects each retailer differently—a furniture retailer is likely to have relatively fewer incidents of ORC than a drug store—it remains difficult to extrapolate ORC estimates to the retail industry as a whole from a limited sample of respondents. In addition to direct losses to retailers, ORC activity can also impact state tax revenues and incur additional costs to consumers. Despite the challenge of developing a reliable estimate of the full economic impact of ORC, researchers and stakeholders generally agree that ORC is a multi-billion dollar issue that affects retailers and consumers nationwide.

Stakeholder roles: A variety of different stakeholders are involved in combating ORC and e-fencing, including retailers, state and local law enforcement, federal entities, and online marketplaces:

- **Retailers:** ORC activity has been identified across a variety of different industry segments and retail outlets of all sizes. Retailers bear the primary impact of these crimes and invest resources to combat ORC activity. Representing individual retailers are several industry groups that are involved in various efforts to communicate ORC-related information and conduct stakeholder outreach and lobbying efforts on behalf of its members. Among these groups are the National Retail Federation, Retail Industry Leaders Association, National Association of Chain Drug Stores, and the Food Marketing Institute.
- **State and local law enforcement:** Local law enforcement is routinely involved in investigating property crimes, including retail theft, but because ORC cases often span across multiple local jurisdictions, investigations may also include county-level or state law enforcement agencies, as applicable. These agencies are generally responsible for enforcing state laws and are routinely involved in developing evidence against potential ORC suspects, which may include surveillance or undercover sales and purchases.
- **Federal entities:** Although there is currently not a federal statute that explicitly criminalizes ORC, such behavior may be prosecuted under a variety of other federal criminal statutes, including, for example, interstate transportation of stolen property, and laundering of

⁷ Richard C. Hollinger and Amanda Adams, *2009 National Retail Security Survey Final Report*, (University of Florida: 2010).

monetary instruments, among others. Principal federal agencies involved in ORC investigations include the FBI and ICE, but may also include the USSS, Postal Service, or Internal Revenue Service if ORC cases involve mail fraud or credit card fraud, among other crimes in which these agencies may have jurisdiction to investigate.

- Online marketplaces: With the introduction of the Internet, online marketplaces have emerged as a powerful platform for commerce for both individuals and businesses alike. However, along with legitimate transactions, such marketplaces also present ORC groups with an additional venue to potentially fence their stolen goods. eBay, founded in 1995, is currently the largest of the domestic Internet marketplaces. The site receives approximately 8 million new product listings daily and includes a combination of product auctions and fixed price sales. Other domestic online marketplaces commonly cited by stakeholders include Amazon, Overstock, and Craigslist. Each of these marketplaces has a distinct business model and they vary considerably regarding the scope of product listings and their level of involvement in the transaction, which may impact efforts related to e-fencing.

Retailers and Law Enforcement Collaborate to Investigate Potential ORC Cases, and Federal Agencies Are Taking Steps to Better Track ORC

Retailers Employ Technology and Personnel to Deter ORC but Must Balance Security Efforts with the Need for Consumer Access to Products

Anyone who has strolled the aisles of a major retailer has encountered retailers' efforts at loss prevention, from electronic tags on clothing to a locked case of iPods. These mechanisms are designed to stop the initial theft, the first step in organized retail crime; however, the effectiveness of these mechanisms is largely unknown, as there is little reported research on the extent, type, and results of any studies that have been conducted to evaluate loss prevention solutions. Additionally, as retailers deploy these theft-detering devices, they must balance the need to secure products with the need to sell them, as products that are too difficult to access

could deter legitimate customers. For example, a customer who needs to locate a sales associate to open a case of iPods may get frustrated and leave a store without making a purchase, resulting in lost revenue for the retailer. In addition, many of these theft deterrents are familiar to customers and boosters alike, and despite retailer efforts, determined thieves often figure out a way to thwart the devices. For example, foil-lined shopping bags—commonly referred to as “booster bags”—can easily render certain electronic sensors useless. Even basic elements, such as a consistent store layout, which can help customers be familiar with any store in a retail chain, can facilitate retail theft by allowing boosters to quickly navigate several stores.

Given boosters’ ability to overcome retailer deterrents, retailers are challenged to develop additional deterrents to ORC, and they continue to experiment with new low- and high-tech solutions. For example, some retailers use specialized displays that dispense one product at a time to prevent an ORC crew from wiping out an entire shelf of a product with a quick sweep of an arm. More high-tech solutions, which one retailer we interviewed is experimenting with, include the use of “enhanced public-view monitors”—motion-triggered recording devices, which begin recording someone as that person reaches into a merchandise display (see fig. 2 for examples of commonly used mechanisms to help detect and deter ORC activity).

Figure 2: Select Technologies to Deter Retail Theft



Locking fixture.



Enhanced public view monitor.



Plastic case securing an individual product.



Electronic article surveillance tag.

Sources: Clockwise from top left: Loss Prevention Research Council, Loss Prevention Research Council, National Retail Federation, and The Kroger Co.

Many retailers are also committed to continued development of new technologies to prevent shoplifting and ORC through the University of Florida's Loss Prevention Research Council (LPRC). LPRC conducts at least 12 research projects per year for the retail industry in an effort to identify new loss prevention technologies that are to be cost-effective in deterring crime. The organization was founded by 10 retailers—including Target, Wal-Mart, CVS, and Home Depot—and retailers currently make up 23 of its 65 dues-paying members. Some current research projects include test and control experiments looking at the effectiveness of the enhanced public view monitors previously described, special protective display fixtures for razor blades, and in-store warning signage.

In addition to new technologies, retailers rely on personnel to aid in their loss prevention efforts. Alert sales associates are one tool for deterring theft, with one ORC expert noting that good customer service is the most recognized theft deterrent in the retail industry. For example, criminals prefer stores where there is minimal interaction with sales associates, allowing them to commit their crimes without drawing much attention. All five of the retailers we interviewed have also invested in loss prevention personnel and asset protection teams designed to investigate theft once it occurs. In general, loss prevention teams vary in terms of size and sophistication depending on the reach of the retailer and the availability of financial resources. These loss prevention personnel can be visible, such as a "receipt checker" who verifies what was purchased as a customer is walking out the door, or behind the scenes, where they monitor surveillance systems inside a store. Retailers and retail chains may also have ORC investigators offsite who work locally and/or regionally to connect the dots between a series of simple shoplifting cases, creating large ORC cases for law enforcement. While there has not been any research conducted to correlate the impact of a dedicated ORC staff on the reduction of ORC activity, one expert noted that it stands to reason that having trained staff would diminish the impact of ORC on a company. See table 1 for a summary of key efforts employed by retailers to help combat ORC.

Table 1: Summary of Select Efforts Employed by Retailers to Combat Organized Retail Crime

Type of effort	Effort description
Technology	<ul style="list-style-type: none"> Security tags <ul style="list-style-type: none"> Electronic article surveillance tags, embedded in or secured to clothing or other products, emit a signal when leaving a store without being deactivated by sales clerk. “Benefit denial” tags typically utilize ink to ruin a product when removed improperly. Radio-frequency identification tags allow retailers to track individual items through the supply-chain, including identifying if they were properly purchased. Locking display cases secure merchandise and must be unlocked by a sales associate to access the product. Specialized displays to dispense one product at a time make it more difficult for a thief to sweep an entire shelf of products. Plastic cases around a single product to secure the merchandise must be removed by sales associate during check out. Camera systems <ul style="list-style-type: none"> Public-view monitors show customers that they are being monitored in the store, recommended for high-theft aisles. Enhanced public-view monitors trigger a recording when someone reaches for a specific product or enters a specific aisle. Closed-circuit television cameras situated throughout a store to record customers and may or may not be monitored real-time by store personnel. Case management systems used to track cases of ORC, including suspects and frequently stolen products, within a retail chain.
Personnel	<ul style="list-style-type: none"> Sales associates whose presence can deter a thief. Receipt checkers who verify that customers leave only with products purchased. Loss prevention personnel who may apprehend boosters in stores. ORC investigators who typically work with law enforcement and other retailers to link incidents of ORC to build larger cases for prosecution.

Source: GAO analysis of retailer information.

As the first line of defense against professional shoplifting, retailers are often the recognized experts in investigating and identifying organized retail crime. Regular exposure to the crime makes it easier for them to differentiate between a shoplifter taking merchandise for personal use and a professional booster. Many retail investigators also have networks that allow them to understand the crimes beyond their specific store or retail chain. Through their dedicated ORC investigators, competing retailers often collaborate on building ORC cases, as ORC groups typically steal common products and hit several different stores in one geographic location in an effort to obtain enough merchandise to fence.

Internal ORC investigators often begin to build cases for law enforcement, as not all law enforcement may have the training to understand ORC or the resources to dedicate to investigating it. In an effort to help increase law

enforcement awareness of ORC, the National Retail Federation sponsors a Joint Organized Retail Crime Task Force, which focuses on developing standard training and awareness programs for retail loss prevention professionals and law enforcement officers. All of the retailers and retail associations we interviewed indicated that retailers usually build complete cases before presenting them to law enforcement. Again, part of this is due to retailers' ability to use their internal networks to identify patterns, but resource constraints on the part of state and local law enforcement also make it difficult for local law enforcement to initiate ORC investigations.

Law Enforcement Agencies Collaborate with Retailers to Investigate ORC, and Federal Agencies Are Taking Steps to Improve ORC Case Tracking

State and Local Efforts

Although retailers play a major role in identifying and developing ORC cases, criminal investigation of these activities largely falls on state and local law enforcement, which typically prosecute retail crimes under state criminal laws. However, four of the eight local law enforcement agencies we spoke with noted that retail theft—and property crime in general—is often viewed as a lower priority than violent crimes. As a result, there are generally limited resources to combat ORC at the local level and any investigations are often conducted on a case-by-case basis, weighing competing resource priorities and the likelihood of successful criminal prosecution. According to several retail and law enforcement stakeholders we interviewed, individual detectives responsible for investigating property crime are often the driving force behind decisions to pursue potential ORC investigations, sometimes due to prior experience with retail theft or pawn shop cases. However, five law enforcement stakeholders noted that there is increasing awareness that ORC is a serious crime—rather than petty shoplifting—and is often linked to other types of criminal activity.

Local law enforcement typically becomes aware of potential ORC cases through retail investigators but law enforcement may also identify suspicious activity, such as the discovery of large quantities of retail merchandise, during routine calls or traffic stops. If law enforcement decides to initiate an ORC investigation, it will routinely work closely with

retailers to develop the case, which may include conducting additional surveillance or undercover “buybacks,” and attempting to “flip” lower level boosters to build a case to higher level entities, as applicable.⁸ If ORC activity spans across multiple jurisdictions, the investigation may be worked in conjunction with other law enforcement entities, potentially to include county or state level resources. For example, one state law enforcement official we interviewed noted that investigators may be able to leverage the resources of specialized units at the county level dedicated to burglary or economic crimes.⁹ According to officials from four of the law enforcement agencies we interviewed, linking multiple retail theft events across jurisdictions is often essential to build an ORC case large enough to be considered for felony prosecution by a district or state attorney’s office. For example, after identifying a similar pattern of thefts occurring across San Diego County in 2008, a detective with the San Diego police department helped establish a task force with law enforcement partners from neighboring jurisdictions to investigate an ORC group suspected of stealing up to \$1 million in merchandise. This group, which was run by two brothers, included a network of highly sophisticated boosters, as well as accomplices who would pre-sort sizes and position merchandise to facilitate theft. The group would routinely target malls in different parts of the county to reduce the chance of law enforcement connecting the events. As a result of the joint investigation, one of the brothers was convicted and 78 individual theft cases were closed. As discussed later, federal entities may also play a role if a retail crime case develops substantially in scope or complexity.

Although retail crime is primarily prosecuted under state criminal laws, the monetary thresholds required for theft to be considered a felony vary from state to state. For example, in Illinois the felony threshold is \$300¹⁰ and in Wisconsin it is \$2,500.¹¹ Retail and law enforcement officials we interviewed noted that professional shoplifters involved in ORC are

⁸ In relation to ORC investigations, undercover “buybacks” generally involve the purchasing of retail merchandise—that is suspected of being stolen—from criminal suspects in order to build evidence of criminal activity. “Flipping” occurs when a criminal suspect chooses to cooperate with law enforcement, such as serving as an informant, generally in exchange for a reduction in criminal charges against them.

⁹ We did not determine the extent to which counties or states had such specialized units since this was beyond the scope of our review.

¹⁰ 720 Ill. Comp. Stat. 5/16A-10.

¹¹ Wis. Stat. § 943.20.

typically aware of these thresholds and often steal at levels below these amounts to reduce the risk of felony prosecution. While two retail stakeholders we spoke with noted that reducing the felony thresholds may provide a limited deterrent to ORC, they also recognized that law enforcement already faces resource constraints with existing retail theft cases. In fact, some states have increased the thresholds in recent years, potentially to focus available resources on higher-priority cases. For example, in Maryland, the state felony threshold has increased twice since 2000, from \$300 to the current level of \$1,000.¹² In January 2011, California also raised the threshold for grand theft in that state from \$400 to \$950.¹³ However, officials in California indicated that prosecutors often try to develop a charge of “conspiracy” or use other criminal statutes, such as those involving false pretenses, in conjunction with major theft provisions to build a stronger case. Similarly, officials we spoke with in Maryland noted that multiple theft incidents may potentially be linked together through the state’s “scheme” statute if substantial evidence exists to identify an ongoing course of conduct,¹⁴ and some other state laws may allow for aggregation of thefts to meet the threshold.¹⁵

In recent years, many states have also developed legislation that specifically targets ORC-related offenses. Examples of provisions outlined in state legislation include defining retail theft and ORC, prohibiting certain high-theft items from being sold at flea markets or similar venues, and establishing felony offenses for multiple thefts occurring within a specified time frame or for specific activities, such as box stuffing or possessing items used for overcoming security devices. Several retail and law enforcement stakeholders noted that ORC statutes in most states are relatively new and, according to three law enforcement authorities we spoke with in states that had ORC laws, there is not yet broad awareness of these provisions by many detectives or prosecutors. As a result, it is too soon to tell what the impact of these statutes may be in terms of providing an additional deterrent to ORC and assisting investigators and prosecutors in building successful cases.

¹² Md. Code Ann., Crim. Law § 7-104.

¹³ Cal. Penal Code § 487.

¹⁴ Md. Code Ann., Crim. Law § 7-103 allows theft committed as part of one scheme or continuing course of conduct to be considered as one crime and the value of the property aggregated for determining whether the theft is a felony or a misdemeanor.

¹⁵ *See, e.g.*, Fla. Stat. § 812.012; 720 Ill. Comp. Stat. 5/16A-10.

Federal Efforts

Although state and local law enforcement are generally responsible for investigating ORC crimes in conjunction with retailers, federal agencies may become involved in major ORC cases that involve a multistate or transnational component. While ORC itself is not a federal crime, it can be comprised of a variety of underlying crimes that can fall under the jurisdiction of multiple federal agencies. As noted previously, the FBI and ICE are the principal federal agencies addressing a range of ORC-related crimes, including interstate transportation of stolen property, money laundering, fraud activities, and aiding and abetting of those crimes, but others may also be involved depending on the case specifics, including investigators with the USSS, Postal Service, and the IRS, among others.¹⁶ Consistent with previous testimony, officials from the three federal agencies we spoke with stated that existing federal authorities and criminal statutes are generally sufficient to target ORC-related activities and groups.

Federal entities typically become aware of ongoing ORC investigations when retail or state and local partners flag these cases for potential federal involvement, or when participating in other collaborative law enforcement efforts, such as task forces. Although officials with FBI and ICE routinely conduct outreach to ORC stakeholders and participate in loss prevention conferences, combating ORC is not an identified mission priority for any of the federal agencies we interviewed, and none has specific resources dedicated to conducting these investigations. This is, in part, because other types of cases are often larger or present a more specific threat to homeland security, such as in the case of terrorism or illegal immigration. In addition, although ORC stakeholders have cited potential links between ORC and terrorism, officials from the federal agencies we interviewed were unable to identify any ORC cases with any specific links to terrorism-related activities or financing.¹⁷ Consequently, decisions to initiate federal ORC investigations are largely conducted on a case-by-case basis, weighing the potential scope and financial impact of the case with other investigative priorities. Retail and law enforcement stakeholders we interviewed also cited factors inherent to ORC investigations that they

¹⁶ Aiding and abetting consists of assisting or facilitating the commission of a crime, or promoting its accomplishment.

¹⁷ Federal agencies and retail associations cite several high-profile cases in which financial profits from ORC groups were transferred to countries known to support terrorism; however, no direct ties between members of these groups and terrorist organizations have been established.

consider when deciding whether an investigation merits the involvement of federal agencies:

- Federal ORC cases are particularly time and cost intensive, often taking several years and potentially requiring \$100,000 or more of retail merchandise to use as evidence. An FBI official responsible for coordinating ORC investigations and a retail stakeholder similarly noted that major ORC cases routinely require extensive undercover and buyback operations to successfully build a case up to the highest levels of an organization.
- Although no specific federal financial threshold exists, stakeholders we interviewed collectively estimated that the value of merchandise stolen required for federal agencies to consider an ORC case ranged from \$100,000 to \$1 million, depending on the jurisdiction. Officials with FBI and ICE also estimated \$100,000 as a likely starting point to pursue federal prosecution, but stated they may review cases with a smaller dollar value of merchandise stolen if it appears that the cases may increase in size or can be connected to other crimes.

FBI: The FBI largely identifies and conducts ORC-related investigations through seven major theft task forces operated in conjunction with other federal, state, and local law enforcement officers. Within the FBI, a total of approximately 55 agents are involved in investigating major theft violations nationwide, some of which are assigned full-time to the 7 major theft task forces located in Chicago, Memphis, New York, El Paso (2), and Miami (2).¹⁸ Agents within these task forces are responsible for working all categories of major theft, which include cargo, vehicle, art, gem and jewelry, and organized retail theft. According to the major theft program coordinator at headquarters, FBI field units in other regions may also initiate an ORC investigation if retailers or local law enforcement present a case to these units or if another federal agency refers a case to them.¹⁹ This official noted that retailers are generally best suited to identify patterns of stolen merchandise, begin theft investigations, and potentially build ORC cases to the point that they may warrant involvement by federal agencies. He stated that the FBI generally determines to initiate a retail

¹⁸ The Special Agent-in-Charge at a field unit is largely responsible for identifying the specific threats and resource priorities for their area of responsibility, which may include allocating FBI personnel to major theft task forces.

¹⁹ It was noted that the major theft program has been reduced in size (through attrition) since 2007 and is now merged with the Violent Crimes Unit.

crime investigation on a case-by-case basis and the decision may be affected by competing threats and other resource priorities. While he is not aware of the FBI turning down any ORC cases that retailers presented, he further stated that cargo theft and vehicle theft likely represent the greatest proportion of cases and the biggest financial impact within the unit.²⁰

According to FBI officials, the primary nexus for bureau involvement with ORC cases relates to the criminal statute prohibiting the interstate transportation of stolen property, a statute that generally applies to stolen goods having a value of \$5,000 or more.²¹ The FBI major theft coordinator noted, however, that the FBI could potentially initiate an ORC case through an investigation of a related criminal activity, including fraud. In this case, a different FBI component may have the lead for the investigation, such as the “white-collar crime” unit. According to the FBI, as of February 2011, the FBI had 531 open cases of interstate transportation of stolen property across the different theft categories. However, officials were unable to identify how many of those cases involve ORC because, until recently, they did not track cases by individual theft categories. As a result, it is unclear to what extent the FBI is using resources to investigate ORC or how the numbers of these cases compare to other major theft categories. Such information would generally be useful to help identify the potential scope of ORC and would provide management with enhanced data with which to make potential resource allocation decisions.

According to the FBI, it recently launched a bureau-wide program that is likely to increase the information available regarding ongoing investigations, including those related to ORC. As of February 2011, the FBI initiated a program across the bureau that is intended to enhance the level of detail of case-related information and improve data collection and reporting efforts. Specifically, personnel are required to use a collection of Crime Problem Indicator (CPI) codes when entering data into the FBI’s case management system.²² The CPI codes include a combination of

²⁰ Industry experts estimate the total losses attributable to cargo theft are as much as \$30 billion per year; however, cargo theft was only recently available as a separate reportable category in the Uniform Crime Report and many companies don’t report cargo crimes. In 2009, the FBI estimated that nearly \$5.2 billion was lost to motor vehicle theft.

²¹ 18 U.S.C. § 2314

²² CPI codes have existed within the FBI for approximately 10 years but utilization was not obligatory across all divisions until the implementation of this program.

mission-oriented threat priorities, as well as case-specific keywords and activity types.²³ For example, ORC-related CPI codes include “organized retail theft” and “infant formula.” According to FBI officials, CPI codes are intended to provide information to unit heads about the threats and crimes being investigated by their agents. If implemented as envisioned, this effort could allow the FBI to mine the case management system for all cases involving ORC. According to the unit chief responsible for overseeing the project, the FBI has put into place a collection of electronic controls, business rules, and operational guidance to help ensure that the codes entered are consistent, accurate, and complete. This official stated that the FBI routinely reviews all ongoing cases every 90 days; therefore, as of May 2011, all ongoing cases would include at least one CPI code. Information from this project generally may be useful to help identify FBI investigative priorities and provide management with additional data on resource utilization—a practice consistent with internal control standards.²⁴ Further, information regarding ongoing ORC cases may serve to better inform ORC stakeholders and Members of Congress of the potential scope and impact of ORC relative to other major theft crimes, which may include identifying whether any additional federal involvement may be warranted. Given that ORC-related cases routinely involve multiple federal crimes and could be investigated by different FBI units, this effort may also be important to help ensure that the major theft program coordinator, or other applicable official, remains fully apprised of ORC investigations being conducted bureau-wide. As the program was only recently implemented and cases are still in the process of being reviewed and updated, it remains too early to tell if these efforts will result in the potential improvements identified.

ICE: ICE has also become increasingly involved in ORC investigations, most commonly when cases include issues related to money laundering, export of stolen goods, or involve crimes committed by suspects residing in the United States unlawfully. ICE is the principal investigative agency within the Department of Homeland Security and its agents have investigative authorities under Title 8, 18, and 31 of the U.S. Code, which

²³ About 1,000 different CPI codes currently exist related to various case-related details, including 24 major threat priorities (as established by FBI management), criminal activities, and individual roles (e.g. financier). Up to 20 different CPI codes can be entered into the case management system.

²⁴ GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD 00-21.3.1](#) (Washington, D.C.: November 1999).

allow them to pursue many different criminal violations that ORC groups routinely commit. According to a senior headquarters official involved in coordinating ORC-related cases, ICE does not dedicate specific resources to investigate ORC cases as they are not an agency mission priority, but it is not uncommon for state and local law enforcement or retailers to contact ICE for assistance in developing cases that involve complex financial or international components. According to ICE, potential ORC cases may be identified through its Cornerstone Outreach Initiative, which is a partnership with the private sector intended to systematically identify and close down vulnerabilities in financial systems through which criminals launder their illicit proceeds. Investigators in one field location also stated that ICE often “backs in” to an ORC case. That is, investigators may be working on an alien-smuggling case and discover that the immigrants are being brought into the country to commit crimes, such as boosting merchandise for an ORC ring. These agents further noted that although a case involves an international component, it may be infeasible for ICE to dedicate investigative resources unless the case is of sufficient scope to merit the attention of a U.S. Attorney’s Office.²⁵ Moreover, given that ICE agents assist in conducting ORC investigations as a collateral duty, their ability to allocate resources may be further affected by other priorities, such as current activities targeting illegal immigration and Mexican drug cartels along the Southwest Border.

Since 2009, ICE has been involved in several initiatives intended to further evaluate its role and enhance efforts related to combating ORC. The ORC Pilot Program, the first of these initiatives, was launched in July 2009, in four cities with known ORC activity: Houston, Los Angeles, Miami, and New York. The program focused on four program areas: (1) development of a database with retail industry contacts; (2) development of a threat assessment to help determine the extent of ORC crimes in which ICE has jurisdiction; (3) enhancing efforts to explore how ORC groups are exploiting vulnerabilities in the banking system to launder profits; and (4) development of a tracking system to assess ICE involvement in ORC cases. In March 2010, ICE extended the program for one year and expanded it to include coordination with the ICE National Cyber Crimes Center, which targets various schemes perpetrated on the Internet, including fraud, money laundering, and selling of credit card or other financial information.

²⁵ ICE officials noted that specific financial thresholds vary but can range from \$100,000 to \$1,000,000 depending on each U.S. Attorney’s Office.

According to program officials, at the completion of the ORC Pilot Program in March 2011, ICE made progress in all key areas identified. For example, ICE affirmed that many ORC cases have an international nexus and can be investigated by ICE special agents, and ICE continues to identify a collection of red-flag indicators of suspicious banking activity related to ORC. In regard to developing a tracking system, ICE created a program code for ORC within its case management system, which is intended to allow headquarters to track case statistics, facilitate identification of potential trends between ORC cases, and help inform resource decisions. During the pilot program, 83 criminal cases were associated with ORC, resulting in 38 criminal arrests, 29 indictments, and 14 convictions. While 14 of these cases were investigated at the pilot program locations, the remaining cases were investigated at 23 additional domestic and international offices in which ICE special agents are located.²⁶ According to ICE officials, these cases have led to the seizure of nearly \$4.9 million in cash, property, and money instruments.

In February 2011, ICE announced the expansion of the ORC Pilot Program into an ongoing national initiative known as SEARCH (Seizing Earnings and Assets from Retail Heists). As part of this announcement, all field units were advised to begin using the ORC program code for all criminal investigations opened under the SEARCH Initiative. Similar to the FBI, ICE supervisors also conduct a quarterly case review, which is intended, in part, to ensure that all applicable program codes are entered. According to ICE officials, the SEARCH initiative will build upon the partnerships with private industry developed as part of the ORC Pilot Program and operates on the assumption that federal anti-money laundering statutes may be among the best mechanisms to target individuals involved in ORC activity. According to ICE, by following the money trail, investigators can often build a case to high levels of a criminal organization. For example, ICE agents were involved in one case in which illicit proceeds from the sale of stolen video games on eBay was tied to an investigation of criminal organizations involved in running the Vietnam underground economy, which included trade in stolen U.S. identities and financial information. In April 2011, ICE indicated that 48 additional cases involving components of ORC had been initiated since the launch of the SEARCH Initiative.

²⁶ Office locations in which at least four individual ORC cases were investigated during this period include Chicago, Dallas, Detroit, Houston (pilot), Los Angeles (pilot), Miami (pilot), Philadelphia, San Francisco, Seattle, St. Paul, and Washington, D.C.

Emerging Regional Networks Are Facilitating Information Sharing among ORC Stakeholders, but Limitations Exist with National ORC Database

Emerging Regional Networks Helping Retail and Law Enforcement Partners Share ORC Information and Build Potential Cases

Given the importance of identifying ORC activity and developing potential cases across multiple jurisdictions, law enforcement entities and retail partners have established regional networks in recent years to facilitate information sharing among stakeholders and potentially identify linkages between connected theft cases. As previously discussed, ORC groups commonly target malls and retail stores across metropolitan areas or even along highway corridors spanning multiple states. As a result of these patterns, a high degree of coordination is required to share suspect information in a timely manner and facilitate the aggregation of multiple thefts into a larger case. A law enforcement official in Florida pointed out that ORC generally requires greater coordination with other state and local law enforcement entities than crimes such as robbery or burglary, which tend to be more localized. To help meet the demand for effective information sharing, a collection of regional networks has emerged in various locales across the country. While each functions independently, these networks commonly identify points of contact and help facilitate identification of ORC suspects and potential linkages between theft incidents. Involvement by federal entities in these regional networks is generally limited as the networks are primarily targeted to retail investigators and state and local law enforcement. However, the networks provide a mechanism with which potential ORC cases can be identified and developed to the point where stakeholders may present them to the attention of federal agencies.

While the specific format and available tools varied between the eight regional networks we studied, they share a number of common elements. For example, all eight of the ORC networks include a contact database of participating retail investigators and law enforcement members, as well as

some type of mechanism to vet individuals requesting membership. The primary outputs for all of these eight networks are informational alerts to participating members when ORC or related theft activity occurs within the region. These alerts commonly include such data as suspect information, incident location, and merchandise targeted. The alerts are intended to be issued in a timely manner after the initial incident so that retailers and law enforcement may be able to detect or deter further theft activity or take additional actions if suspects are identified in another location. As table 2 indicates, the ORC networks we identified range from relatively basic technology platforms, such as Google Groups, to stand-alone websites that incorporate more advanced tools, such as maps indicating locations of recent theft incidents, customizable alerts, and keyword searching to identify incidents matching selected criteria. As an additional component, members of six of the regional networks also hold periodic meetings or annual conferences to discuss ORC-related trends and activities.

Table 2: Characteristics of Selected Regional Networks Targeting Organized Retail Crime

Organized retail crime network	Key characteristics
Albuquerque Retail Assets Protection Association (ARAPA)	<ul style="list-style-type: none"> Initiated in 2008 — approximately 374 members. Site includes member directory, incident reporting forms and customizable incident alerts, and incident mapping and searching tools. Approximately 30 theft incident alerts issued per week. Association includes monthly member meetings.
Los Angeles Area Organized Retail Crime Association (LAAORCA)	<ul style="list-style-type: none"> Initiated in late 2009 – approximately 500 members. Site shares same technology platform and capabilities as ARAPA – approximately two theft incident alerts issued per day. Dedicated individual available to field inquiries and provide ORC expertise. Another individual monitors alerts to identify potential connections to other crimes. Association includes member meetings every 6 weeks.
Bay Area Organized Retail Crime Association (BAORCA)	<ul style="list-style-type: none"> Initiated in May 2010 – approximately 378 members. Site shares the same technology platform and capabilities as ARAPA and LAAORCA. Approximately 8-10 theft incident alerts issued per week. Member meetings occur every 3-4 months and often include case presentations.
San Diego Organized Retail Crime Association (SDORCA)	<ul style="list-style-type: none"> Initiated in October 2010 – approximately 180 members. Includes member database and standardized incident report form. Approximately five theft incident alerts issued per week. Individual at San Diego Police Department vets members and responds to requests.

Organized retail crime network	Key characteristics
Cook County Regional Organized Crime Task Force (CCROC)	<ul style="list-style-type: none"> Initiated in December 2010 – approximately 500 members. Site shares same technology platform and capabilities as other networks (ARAPA, LAAORCA, BAORCA), as well as advanced analytical tools, such as identified linkages between suspects. Ad-hoc meetings occur as needed to discuss ongoing investigations and an annual symposium is to be held in 2011. Individual within Cook County State Attorney's Office vets members and responds to requests.
Florida Organized Retail Crime Enforcement Network (FORCE)	<ul style="list-style-type: none"> Utilizes Google Groups as central repository of member contacts and for email distribution of incident alerts. Approximately 800 members. Network includes monthly meetings of approximately 20-30 members and a larger annual meeting.
Metropolitan Area Law Enforcement/Loss Prevention Retail Crimes Networking Group (Pennsylvania, Maryland, D.C., Virginia)	<ul style="list-style-type: none"> Established between 2004/2005 – approximately 200 members. Consists of email distribution list to submit alerts, suspect information, and other theft incident information. Detective within Montgomery County Police Department (Maryland) vets all new members and all alerts before distribution to members.
Washington State Organized Retail Crime Association (WSORCA)	<ul style="list-style-type: none"> Scheduled implementation in May 2011 – ongoing vetting of participating retail and law enforcement members throughout Washington and Oregon. Site shares same technology platform and capabilities as other networks (ARAPA, LAAORCA, BAORCA).

Source: GAO analysis of information from local law enforcement agencies.

All of the law enforcement stakeholders we interviewed recognized the regional networks as an important tool to consolidate ORC stakeholder contacts and share information among members in a timely manner. According to three law enforcement officials we spoke with, these types of regional networks can be particularly helpful because—through the theft incident alerts—investigators may identify suspects who are wanted for other potential crimes. As a result, these networks may help ensure that multiple cases involving the same individuals are linked together to better leverage resources and avoid duplication. In Albuquerque, for example, a law enforcement official stated that hundreds of cases have been linked through the information-sharing network in that region since its inception in 2008, including one involving a retail-theft ring connected to over \$400,000 in stolen merchandise.

To date, individual law enforcement agencies have taken the lead to develop these regional networks but retailers have played a major support role and, in some cases, have served as the primary funding sources for site development and maintenance. While some regional networks have taken advantage of free technology platforms such as Google Groups, more developed networks have entailed dedicated funding and contractor

support. For example, the Los Angeles Police Department fully funded the initial development of the LAAORCA system, which was among the regional networks that we reviewed with more advanced capabilities. However, this project included participation from major retailers, as well as the National Retail Federation. Although the Los Angeles Police Department provides the majority of funding for ongoing operation of the network, a non-profit entity was established to receive financial support from members to help fund ongoing meetings and conferences. More importantly, it appears that other law enforcement agencies may be able to build upon the success and investment of the regional networks already established. For example, a law enforcement official responsible for establishing the BAORCA system in Northern California noted that he worked with the same contractor that developed the networks in Albuquerque and Los Angeles, and was able to utilize the same technology platform for minimal development cost. According to this official, the BAORCA network was developed and implemented for less than \$2,000 plus additional annual operating and maintenance costs of approximately \$1,500. Initial and ongoing costs have been fully supported by four member retailers. The Cook County State Attorney's office was similarly able to utilize existing technology platforms to develop its Web site, for which initial funding was provided by Target. These examples illustrate the potential to leverage resource investments and an opportunity to develop partnerships between law enforcement agencies and retail stakeholders to help sustain these regional networks in the longer term.

LERPnet Provides a Mechanism to Share Data Nationally, but Stakeholders Report That Use of the Database by Retailers and Law Enforcement Has Been Limited

As part of the Violence Against Women and Department of Justice Reauthorization Act of 2005, the Attorney General and the FBI were required to establish a task force to provide expertise to the retail community for the establishment of a national database, to be housed and maintained in the private sector and to track and identify where organized retail theft crimes occur.²⁷ According to the legislation, the national database was to allow federal, state, and local law enforcement officials, as well as authorized retail companies, to transmit information into the database and review information that was submitted electronically. According to the statement of the amendment's sponsor, the database was, among other things, intended to help provide federal law enforcement with information illustrating the interstate nature of organized retail theft

²⁷ Pub. L. No. 109-162, § 1105, 119 Stat. 2960, 3092 (2006).

crimes.²⁸ While funds were authorized in the act for activities related to federal efforts to combat organized retail theft and for working with the private sector to establish and use the database, no money was ever appropriated under this section. Despite the lack of federal funding, a working group was established—comprised of the FBI and three major retail associations—to move forward with the development of the database. One retail association, NRF, ultimately took ownership of the project and provided the sole funding for the creation of what became known as the Law Enforcement Retail Partnership Network (LERPnet). LERPnet became operational for retailers in 2007 and was linked to Law Enforcement Online (LEO.gov) in January 2010, which provided access to all federal, state, and local law enforcement officers.

Despite initial support, none of the five retailers we interviewed found LERPnet to be a useful system for sharing information and identifying trends related to ORC. Two retailers told us they discontinued their membership in LERPnet because it did not provide a sufficient return on investment.²⁹ A major retailer, which continues to support LERPnet, further indicated that its internal data along with regional information-sharing networks have generally been more useful than LERPnet in investigating ORC. While all five indicated that they believed in the goal of LERPnet as a way to share information, some felt it lacked sophisticated analytics to help retailers identify trends and standardized data entry (each retailer chooses what information to enter). Retail stakeholders indicated analytical tools to help identify national-level ORC trends and patterns would be useful, helping to connect suspect information. Local law enforcement officials we interviewed also indicated that LERPnet was not widely used to facilitate their investigative efforts. Specifically, officials from eight of the local law enforcement agencies stated that they rely primarily on regional information-sharing networks as their cases are typically regional in nature. According to these officials, the regional networks are most relevant to local law enforcement because they are specifically targeted to the investigative area and bordering jurisdictions and provide real-time updates.

In April 2011, LERPnet was acquired by ISO Crime Analytics, a data-management company with experience running large information-sharing databases for the retail, insurance, and banking industries. LERPnet 2.0, as

²⁸ H.R. Rep. No. 109-233, at 97, 624-25 (2005) (statement of Rep. Goodlatte).

²⁹ Annual dues are based on a company's annual sales.

it is being called, is intended to address some of the criticisms leveled at the original LERPnet when it becomes operational sometime in the summer of 2011. For example, the system is to have link analysis tools to help identify potential patterns of criminal activity and enhanced notification mechanisms for retailers. Additionally, ISO Crime Analytics is planning to hire a full-time data analyst to supplement the automatic tools. Working with a retail advisory board of 15 to 18 members, ISO Crime Analytics is to address standardization of data entry, including providing uniform definitions to aid in consistent reporting of incidents. The company is also working to simplify data entry of theft incidents, in part, by further enabling direct uploads from retailers' existing case management systems. While the CEO of ISO Crime Analytics acknowledged that it will take time for the alerts to be "real-time," the goal is to get incident information uploaded into the system as quickly as possible to enhance alerts available to retailers and law enforcement that want to receive them. LERPnet 2.0 will be capable of linking to other crime databases such as the National Crime Information Center, but the specific databases are to be decided by the retail advisory board, which the company said was to be formed in June 2011.

ISO Crime Analytics indicated that the system is first and foremost a retail tool, since retailers are the entities most responsible for identifying stolen product, inputting incident details into LERPnet, and using that data to make links with other retailers and build potential ORC cases. An FBI official responsible for coordinating ORC investigations similarly stated that retailers are best suited to use LERPnet to help identify patterns of ORC activity, make links between stolen merchandise and goods being sold online, and identify major cases that may merit federal involvement. For example, one retail investigator noted that certain brands or products may be store-specific, making individual retailers the most appropriate stakeholder to identify which of those products could be potentially fenced online. The FBI official further indicated that the value of LERPnet is in making it easier for retailers to aggregate cases—thus demonstrating a bigger impact with a federal nexus—and that the agency typically relies on retailers to bring them ORC cases because of the FBI's limited resources and other threat priorities. He noted that once an ORC case is presented to the FBI for potential involvement, agents would be able to use the FBI's internal case management system to identify if any other cases involving the same criminal suspects or organizations were open nationwide, potentially linking ORC to other crimes. ISO Crime Analytics hopes that the new system will also eventually be of use to local law enforcement. For example, a company official noted that law enforcement may benefit from retailer alerts for areas within their jurisdiction or could

potentially match stolen goods discovered to reported thefts. Since LERPnet 2.0 has yet to become operational, it is unclear how widely it will be used by law enforcement.

Leading Online Marketplaces Have Taken Steps to Combat e-Fencing, but It Is Unclear If Additional Federal Action Is Warranted

eBay, the Largest Online Marketplace, Has Recently Taken Steps to Deter e-Fencing, but Varying Business Models and Available Resources Impact Efforts of Other Online Marketplaces

eBay

Recently eBay, the largest online marketplace, has begun a series of efforts designed to prevent the sale of stolen merchandise on its site. The site maintains a “prohibited items” list designed to prevent the sale of items subject to federal regulations—including firearms, alcohol, and tobacco products—and other items unlicensed for sale, including stolen property. However, eBay’s recent efforts have been designed to make it more responsive to requests for information from both retailers and law enforcement, both of which usually need seller information from eBay to link stolen merchandise to specific people. Prior to its recent efforts, eBay provided seller information to retailers and law enforcement when it was legally required to do so through a subpoena, or other appropriate legal

process.³⁰ In early 2008, eBay began to change its approach to the issue of ORC, recently developing a series of initiatives designed to more easily provide information to retailers and law enforcement alike.

For retailers, eBay developed the PROACT program, providing a way for retailers to quickly submit and receive information on eBay sellers they suspect of selling stolen merchandise. The program currently has 300 members. All retailers can submit a request for information on a seller to eBay, and as of January 2011, eBay had received 2,340 requests for information.³¹ eBay's PROACT investigators can provide information requested, such as name, address, and seller history.³² eBay PROACT investigators may also help retailers with their investigations by providing them with an undercover account, which may be used to purchase merchandise they suspect is stolen to help build a case, linking confirmed fraudulent sellers—"bad actors," in eBay terms—to other users or accounts, and taking action on user accounts, such as suspending them or pursuing criminal action against them in concert with retailers and law enforcement.

eBay also provides retailers with:

- eStop: On every product page, eBay has placed a "Report Item" link, providing a mechanism to report a listing violation, including stolen property. eBay has indicated eStop has been used three times since it was implemented in early 2010. However, eStop requires retailers who want a listing removed to affirm that the specific listing is stolen. Often, they cannot make this affirmation without additional information about the seller from eBay, which is one of the reasons why eBay believes the tool has been used infrequently.

³⁰ eBay stated that the company has always maintained ways for law enforcement to obtain information through requests on department letterhead, court orders and LeadsOnline, which is described later.

³¹ The disclosure of personal user information to retailers and law enforcement is covered in eBay's privacy policy, which indicates that relevant information may be disclosed in response to a verified request related to a criminal investigation or alleged illegal activity.

³² eBay will not provide PayPal information, as eBay noted that banking information requires a subpoena from law enforcement. PayPal, which was acquired by eBay in 2002, allows consumers to make or accept payments online without directly exchanging financial information.

-
- Exception reporting: For PROACT member retailers, eBay is to create customized “exception reporting” for those who request it. eBay will work with these retailers to build reports on products frequently stolen from their stores. As of May 2011, eBay has created these reports for nine retailers. The reports provide retailers with information showing the top suspicious sellers of high-risk items based on quantities, price points, and high-theft areas. One retailer we interviewed uses these reports to identify sellers that warrant additional investigation—internally and within eBay—to determine if the products that are being sold have been stolen from their stores.

eBay has also created tools to aid in providing law enforcement with access to information. eBay’s Law Enforcement Portal allows state, local, and federal law enforcement to request information from eBay on users suspected of selling stolen merchandise. The company allows all vetted LE agencies to use the Portal to investigate possible illegal activity on the site, including the sale of stolen goods, and eBay reviews all requests to ensure they comply with eBay’s privacy policy. According to eBay officials, it approves about 99 percent of requests, responding within 48 hours with the name, address, Internet Protocol (IP) and email addresses, any additional contact information, shipping information, listing and sales data, and user history over the last 2 years.³³ In 2010, eBay received 603 requests through the portal. eBay also built the Law Enforcement eRequest System to allow law enforcement to submit requests for information and court orders electronically. Since inception in November 2010, 1,601 requests or court orders have been submitted by law enforcement in North America. Additionally, all law enforcement can access eBay information through LeadsOnline, an online, property-crimes database. eBay provides access to listing and sales data through LeadsOnline automatically, providing law enforcement with another investigative tool. Through the database, law enforcement users of the system can get basic seller information from the past 3 months. In 2010, 2,090 law enforcement agencies conducted 12,990 eBay related searches on LeadsOnline. For more detailed information, law enforcement agencies are to contact eBay directly.

In addition to its retail and law enforcement efforts, eBay has also implemented and improved a series of procedures designed to verify seller information, proactively flag suspicious listings, and further protect

³³ An IP address provides information on the specific name and location of a computer.

buyers. These efforts are independent of retailer or law enforcement requests. These efforts include:

- Enhanced seller vetting: Starting in October 2010, eBay verifies users' names, addresses, and phone numbers, and restricts new seller activity until the seller builds a good business record on eBay.³⁴
- Filters: eBay utilizes thousands of rule-based filters that search for suspicious listings. Filter variables can be seller based (financial, user information, feedback), item based (category, pricing, keywords), or risk based (internal losses, risk models).
- Exception reporting: eBay runs 17 monthly exception reports on over 100 categories of commonly stolen products such as gift cards, health and beauty aids, and infant formula. These reports are designed to identify sellers who may have a high volume of sales in several retail high-theft categories for further review or monitoring by eBay. From January 2010 through March 2011, eBay has proactively reviewed 490 sellers, 237 of which were deemed "bad actors," compared with 2,870 requests received from retailers and law enforcement, 220 of which were deemed "bad actors."
- Payment holds: Through PayPal, eBay has instituted a 21-day hold on funds to new accounts so that proceeds from the sale of merchandise are not available until the hold expires. eBay believes this is an effective deterrent to the listing of stolen merchandise online as thieves generally look for a quick way to convert merchandise into money.
- Seller messaging: To remind sellers of eBay's rules related to certain products, such as infant formula, eBay provides specific messaging if a seller is trying to list the product. For example, sellers of infant formula are reminded that they must include the expiration date of the formula in the listing and that it is against eBay's policies to sell expired infant formula. These efforts are intended to protect consumers from purchasing potentially expired products but may also provide an additional deterrent to those knowingly selling expired products.

³⁴ eBay officials also noted that the company has a program in place to ensure that buyers are protected in the event that they do not receive an item purchased or the item is not as described.

Retailers and law enforcement alike indicated that eBay's recent efforts have been effective at facilitating information sharing during ORC investigations. Three of the 5 retailers and 6 of the 10 state and local law enforcement agencies we interviewed are members of their respective eBay programs, as are members of FBI and ICE. Several indicated that the company is timely and effective in providing requested user information, and both groups commented that eBay's commitment to information sharing is a significant change from a more contentious relationship previously. eBay's recent efforts to increase its cooperation with retailers and law enforcement have been voluntary on the part of the company. Several retailers, and eBay itself, credited its Senior Director of Global Asset Protection—an individual with a retail loss prevention background—with developing the more open environment at eBay. Two retailers we interviewed—one PROACT member and one non-member—as well as two retail associations, cited specific concerns about eBay's maintaining its long-term corporate commitment to the PROACT program. In response, eBay officials reiterated the company's long-term commitment to PROACT, noting that the program maintains buy-in from senior corporate officers and is part of a larger effort to enhance working relationships with retailers.³⁵

Other online marketplaces

While eBay is the domestic online marketplace most commonly cited by stakeholders, other online marketplaces, such as Amazon.com, Overstock.com, and Craigslist, could also be potential outlets for stolen merchandise. Like eBay, these marketplaces forbid the sale of certain goods on their sites and, to varying degrees, undertake some review of listings. However, these other marketplaces operate differently and some do not have the resources nor conduct the volume of transactions as eBay, which could make it difficult to implement the kinds of initiatives that eBay has started. For example, Amazon.com and Overstock.com are primarily online retailers, directly selling goods to consumers. In addition to selling directly, these sites offer a way for other merchants, individuals or small "storefronts" to sell to their customers. This sales stream accounts for approximately 30 percent of units sold on Amazon.com in

³⁵ In responding to a draft copy of this report, eBay officials also noted that the company has formed several partnerships intended to help combat ORC, including those with NRF, FMI, the Jewelry Security Alliance, and the National Association for Shoplifting Prevention. Examples of specific efforts conducted through these partnerships include the establishment of a working group with retail stakeholders to address ORC issues and a campaign to provide community resources for shoplifting prevention education and information.

2010 and about .5 percent of Overstock.com's overall business. Even though these third-party sales are not their primary business, both Amazon and Overstock have taken steps to ensure the integrity of their sites. All sellers on Amazon must first register with the site, providing name, address, and an active credit-card number. In addition, sellers must provide a telephone number to finalize registration, which is only complete when a personal identification number is entered during a call to the given number. In certain product categories—such as clothing and accessories, electronics, and watches—Amazon limits the addition of new sellers and closely monitors their performance to ensure products are delivered in a timely manner and in the condition described. According to Amazon, the company guarantees the condition of the item and its timely delivery when customers purchase products through third-party sellers on its site. Amazon also monitors the rates of customer complaints, claims, disputed credit-card transactions and other metrics in an effort to ensure that sellers are maintaining a high standard of fulfillment and customer service. Sellers who fail to meet performance requirements are blocked from selling. In addition, Amazon has security processes in place to flag suspicious activity, which may include changes in seller activity. Furthermore, like eBay, all new sellers on Amazon are subject to payment holds. Amazon disburses seller funds every 14 days.

Like Amazon, Overstock requires registration from all buyers and sellers, and verifies registration details through a credit card verification process, affirming that the registrant reported information matches credit-card-billing information. In addition, the company officials stated that staff manually reviews listings, going through every listing category daily looking for fraudulent auctions. When Overstock flags suspicious listings, it is to request proof of ownership of the offered goods from the seller. As with Amazon and eBay, Overstock also places limits on the amount of product being sold by new sellers until they have established a favorable seller rating. Both Amazon and Overstock indicated that they are willing to work with merchants and law enforcement partners as needed to address potential e-fencing activities, and they have done so in the past.

Law enforcement from four local agencies, three retailers, and one retail association also indicated that some criminals are using Craigslist to sell stolen merchandise, and some of them would like to see increased information sharing from the site. However, Craigslist provides an online classifieds service which functions similarly to the classifieds sections of newspapers. As such, Craigslist provides a service through which sellers of goods can meet potential buyers, but—as with newspaper classifieds—Craigslist has no involvement in any actual transaction. Craigslist does not

charge for listings in its “for sale” categories, nor does it make any money from a completed transaction, should one occur.³⁶ Since buyers and sellers deal with each other directly, company representatives noted that there is no way for Craigslist staff to know whether any transaction—lawful or unlawful—has even occurred. Additionally, Craigslist does not require registration to use its site and does not collect personal information, such as name or address, about the seller who posts an item for sale. According to the company, its 32-member staff could not reasonably vet sellers, as it receives approximately 1 million free “for sale” listings each day. Given the overall volume of listings, Craigslist representatives indicated that they feel illegitimate use of the site is rare. However, the company does provide a flagging feature on every ad, so that Craigslist users can flag ads that appear problematic. Ads receiving a sufficient number of flags are automatically removed. Craigslist also captures some electronic information, such as IP address and email address, which Craigslist provides to law enforcement when served with appropriate legal process, such as a subpoena.³⁷

Each of the four internet marketplaces that we reviewed, including eBay, prohibits a range of specified products from their sites. Some of these prohibitions are due to federal regulations, such as those related to the sale of firearms, alcohol and tobacco products, or other items unlicensed for sale in the United States. However, other voluntary product restrictions may be identified in each site’s internal policy guidelines, and the development and implementation of these policies is generally at the discretion of the individual marketplaces. While all of the online marketplaces that we reviewed utilize a combination of mechanisms to identify policy breaches, including technology filters, it is unclear to what extent other existing or emerging marketplaces will also implement such efforts, potentially leaving them vulnerable to being used for e-fencing.

³⁶ Craigslist offers local classifieds and forums with listings on, among other things, items for sale, jobs, housing personals, and local events. Listing on Craigslist is free, except for job postings in 19 cities, brokered apartment rentals in New York, and therapeutic services throughout sites in the United States.

³⁷ Craigslist indicated that applicable law, including the Electronic Communications Privacy Act (ECPA), does not allow it to provide information about a specific listing to government authorities without a subpoena, except in rare exigent circumstances. ECPA regulates the disclosure of electronic communications and subscriber information by electronic communication service providers and remote computing service providers. Among other things, ECPA generally requires that law enforcement obtain appropriate legal process, such as a search warrant or subpoena, in order to obtain subscriber information—such as a name or IP address—from a provider. 18 U.S.C. § 2703.

Stakeholders Identified
Additional Federal Actions
Intended to Deter e-
Fencing and Mitigate
Potential Health and Safety
Concerns but Potential
Impacts Are Unknown

Seller Contact Information

Retail and law enforcement stakeholders we interviewed identified two options that could help combat ORC, but both would require legislative action to implement and the potential impact remains unknown. The first, proposed by two retailers and representatives from three retail associations we spoke with, would require that identified high-volume sellers on online marketplaces list a verified name and address, viewable to potential buyers.³⁸ According to one retailer, this initiative would be intended to provide an additional deterrent to e-fencing by reducing the perception by sellers of anonymity during online transactions. Determination of high-volume sellers could be based on sales volume or the number of completed transactions in a specified time period. However, officials from online marketplaces we interviewed identified several potential concerns with such a requirement and it is not known to what extent it would deter those engaged in e-fencing activities.

Specifically, officials from eBay stated that providing potential buyers with seller contact information may undermine its business model by allowing buyers to circumvent the site and contact sellers directly. Similarly, Amazon officials noted that making this information public is currently prohibited by the company's terms and conditions and emphasized their desire to avoid any potential efforts by customers to circumvent Amazon and pursue direct sales from merchants. Further, eBay company officials noted that providing public access to seller information may also present a potential safety risk as specific merchandise, its estimated value, and its location would be available to potential criminals, a safety concern that Amazon officials echoed. Finally, eBay officials voiced concern that

³⁸ Two bills proposed in the 111th Congress included such a requirement—S. 470 and H.R. 1173—which respectively defined high volume sellers as those that engaged in (1) discrete transactions totaling an aggregate value of \$12,000 or more during a 12-month period; or (2) 200 or more transactions with an aggregate total of \$5,000 or more; or as a seller on an online marketplace who in the past 12 months has made or offered to make discrete transactions aggregating at least \$12,000.

providing full contact information, particularly an email address, may present an increased risk to sellers of identity theft due to the greater potential for “phishing” scams.³⁹ These concerns would likely also apply to other online marketplaces with similar business models that cater largely to individual sellers. In addition, as discussed previously, eBay already conducts a number of actions to validate sellers on its site and collects a great deal more seller information than such a requirement would provide, information that the company makes available to retailers and law enforcement as requested.

In accordance with e-commerce legislation in the European Union (EU), designated business sellers operating on a range of e-commerce sites, including eBay-operated sites in that region, are obligated to list full contact information, which is to include name, physical address, and an e-mail address.⁴⁰ However, according to eBay officials, business seller laws do not contain a consistent legal definition of what constitutes a business and the legal obligation for properly identifying themselves as either a business or a consumer lies exclusively with the seller. eBay provides its sellers a means for this designation on its marketplace sites and informs them of their statutory duties, but generally does not make this determination and has no reporting requirements to EU or national agencies regarding sellers’ compliance. However, eBay officials indicated that above a very high threshold of sales, eBay may require sellers to register as a business (subject to a right of appeal) on some of its European sites. eBay officials further noted that applicable business seller laws instituted in some EU countries were developed as one component of a broad consumer protection framework present in the EU and were not connected to the issue of e-fencing. According to eBay officials, as it is unlikely that sellers engaging in e-fencing would self-identify as a business, the requirement would not likely be effective as a means to compel

³⁹ “Phishing” is a fraudulent practice intended to induce individuals to reveal personal information, such as usernames, passwords, or credit card details by falsely purporting to be a trustworthy entity in an electronic communication.

⁴⁰ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Among other things, the law requires contact information to be provided by “information society services,” which includes, for example, online information services (such as online newspapers), online selling of products and services (books, financial services and travel services), online advertising, professional services (lawyers, doctors, estate agents), entertainment services and basic intermediary services (access to the Internet and transmission and hosting of information).

criminals to provide their contact information. eBay officials in the EU also reiterated that buyers in that region often contact sellers directly in an attempt to circumvent eBay seller fees—a practice they noted that puts buyers at increased risk of loss and other fraudulent activity. Further, eBay officials noted at least one verified case in which a seller was attacked in their home when selling high-value luxury goods as a business seller on eBay in the EU. Given the concerns identified, it is unclear if instituting such a requirement in the United States would serve as an effective mechanism to deter ORC groups from using the internet to fence stolen goods and not result in unintended negative consequences. Further, given that law enforcement agencies can already request seller contact information from online marketplaces through other means, including through eBay’s Law Enforcement Portal or through legal process, such as a subpoena, these agencies’ ability to investigate potential e-fencing activities would not be affected by such a requirement.

Selected Product Restrictions

Given the potential health and safety concerns related to ORC cited by three major retail associations and three law enforcement stakeholders, the second option for legislative action they identified relates to the potential restriction of selected products from online marketplaces or other identified fencing locations, such as flea markets. These restrictions would likely target the most common products of concern identified by stakeholders, including infant formula, over-the-counter (OTC) medications, and other applicable health and beauty products. However, it is not currently known if the second-hand sale of these goods has actually resulted in a public health problem. For example, an investigator with the U.S. Department of Agriculture stated that although there are routinely major cases involving the sale and redistribution of stolen infant formula, he was not aware of specific health impacts resulting from these products. Further, any potential ban on the sale of specific products would also impact the legitimate sellers conducting business in online marketplaces or other venues.

Four of the ten law enforcement officials we interviewed indicated that OTC medications and other health and beauty products are commonly fenced via swap meets and flea markets, as well as through privately owned convenience stores and online marketplaces.⁴¹ As a result, there is

⁴¹ This issue was not discussed in all of the interviews conducted with law enforcement officials, and based on the individual roles and experiences of these officials, some could not comment specifically on the scope or impact of this activity.

limited assurance that these products were lawfully acquired and are stored and handled according to the manufacturer's recommendations. Two of the four retail associations we interviewed noted that their members routinely work directly with manufacturers of these products, which provides the retailers with increased assurance that products are stored and handled properly and that they would be informed in a timely manner in the event of a recall. At least one state has already passed legislation restricting a targeted list of high-theft health and beauty products from being sold at flea markets and similar public venues without proof of ownership.⁴²

If additional sales restrictions for these venues were implemented at the federal level, a range of potential actions could be considered, including a complete restriction on the sale of specified products through select sales channels, or requirements to provide additional information in product listings in online marketplaces, such as the manufacturing lot number and any applicable expiration dates. Such information may provide additional assurance to buyers and allow them to determine if any of the products may be subject to recall.⁴³ For example, eBay has instituted a requirement that sellers clearly list the expiration dates for all infant formula within the product description. Yet, lacking any identifiable public health impacts to date, it is unclear whether or not any such actions to restrict specified healthy and beauty products are warranted.

Agency Comments and Our Evaluation

We provided a draft of this report to DOJ and DHS for official review and comment. DOJ did not provide comments and DHS written comments are contained in appendix I. We also provided selected excerpts of the draft report to eBay, Amazon, Overstock, and Craigslist to obtain their views and verify the accuracy of the information provided. We incorporated their technical comments into the report, as appropriate.

⁴² Colo. Rev. Stat. § 18-13-114.5 places restrictions on the following items: baby food, cosmetics, medical devices, drugs, infant formula, batteries, and razor blades.

⁴³ OTC medications and other products subject to recalls are listed on an FDA website at <http://www.fda.gov/Safety/Recalls/default.htm> and are typically identified by the product lot number.

We are sending copies of this report to the Attorney General, the Secretary of Homeland Security, and other interested parties. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report or wish to discuss the matter further, please contact me at (202) 512-8777, or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Sincerely yours,

A handwritten signature in black ink that reads "Eileen Regen Larence". The signature is fluid and cursive, with the first name "Eileen" being the most prominent.

Eileen Regen Larence
Director, Homeland Security
and Justice Issues

Appendix I: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

May 31, 2011

Eileen R. Larence
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-11-675, "ORGANIZED RETAIL CRIME: Private Sector and Law Enforcement Collaborate to Deter and Investigate Theft"

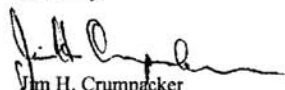
Dear Ms. Larence:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security appreciates the U.S. Government Accountability Office's work in planning and conducting its review and issuing this report.

The Department is pleased to note the report's positive acknowledgement that U.S. Immigration and Customs Enforcement (ICE) is one of the principal federal agencies addressing a range of Organized Retail Crime (ORC)-related crimes. In addition to participating with other law enforcement agencies in developing cases that involve complex financial or international components, ICE has been involved in several initiatives intended to further evaluate its role and enhance efforts related to combating ORC. For example, last year ICE expanded its efforts to include coordination with the ICE National Cyber Crime Center, which targets various schemes perpetrated on the Internet, including fraud, money laundering, and selling of credit card or other financial information. Although combating ORC is not an ICE mission priority, ICE will continue to support these types of investigations on a case-by-case basis, as appropriate.

Once again, thank you for the opportunity to review and comment on this draft report. Technical comments on the draft report have been provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Eileen R. Larence, (202) 512-8777, or larencee@gao.gov

Acknowledgments

In addition to the contact named above, Kirk Kiester, Assistant Director, and Ryan Lambert, Analyst-in-Charge, managed this assignment. Erin Henderson, Jessica Orr, and Janet Temko made significant contributions to the report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

